December 21, 2005

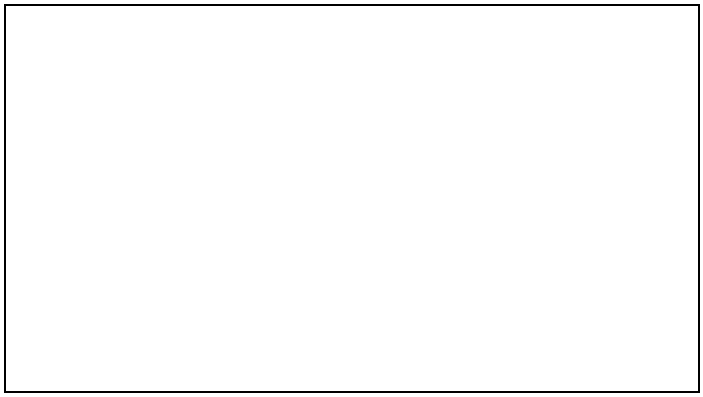
Dear Community Friends:

Gone "Phishing"

If you are not familiar with the term, "Phishing" scams are where you get an email that appears to be from a bank, financial institution or other entity. The email asks you to click on a link to update or verify your account information because of some sort of compromise to your account or software problem. Many of these sites and emails look authentic and are convincing enough to make you think it is the real deal. The purpose is to get your account information and Personal Identification Number (PIN) so they can raid to their hearts content and use your identity to perpetrate further crimes. Additionally, some of these sites infect your computer with viruses.

Here's an example of a Phishing email:

Subject: Regions Bank alert: unauthorized login attempts



I've gotten a ton of these myself, from PayPal, SunTrust, Citibank, Washington Mutual…. I knew they were scams because I don't have accounts with ANY of them. Also, if my financial institution has an issue with my account, they call, not email (and trust me, they've called).

So what should you do? Simple: **Hit Delete**. Do not respond to the email and DO NOT click on the link, especially if you do not have an account with that financial institution.

If you have clicked on the link, followed the instructions and now feel that your information has been compromised, definitely alert your bank, credit card company or whatever financial institution is applicable. And don't do it again.

We've also received reports of an email scam disguised as a patch for McAfee products. You may receive a spoofed email message instructing you to click on a link to download and install a patch from McAfee. The link in the email takes you to a fraudulent website, that appears to be the legitimate McAfee security site. If you receive this email, please delete it; do not click on the link.

Typically vendors do not distribute emails that direct end-users to a website link for software updates. Anyone receiving this type of email at home or at work should be extremely suspicious and verify the sender before following any instructions contained in the email.

For additional details and information on how to detect and prevent this type of attack: http://www.websensesecuritylabs.com/alerts

All Our Best to You and Yours

On behalf of the officers, detectives, coordinators, command staff and support staff of the South Precinct; we wish you Merry Christmas, Happy Hanukkah, Blessed Solstice and Happy Kwanzaa. May the New Year bring you happiness, health, prosperity and joy.

Take Care and Stay Safe!

Mark Solomon
SPD South Precinct Crime Prevention